

1/5/6 (Item 6 from file: 351)  
DIALOG(R) File: 351:Derwent WPI  
(c) 2004 Thomson Derwent. All rts. reserv.

011377311 \*\*Image available\*\*  
WPI Acc No: 1997-355218/ 199733  
XRPX Acc No: N97-294553

**Interactively managed information providing method for access control of communication service through computer network - involves evaluating propriety of information and not accepting provision of information when effective term of interactive identifier expires**

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE )

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 9146824	A	19970606	JP 95307231	A	19951127	199733 B

Priority Applications (No Type Date): JP 95307231 A 19951127

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 9146824	A		8		

Abstract (Basic): JP 9146824 A

The method involves the connection of a server computer (102) which has world wide web to a client computer (101) in a network (103). Information is provided from the client computer to the server computer using a hypertext transfer protocol. A judging unit judges whether an information acquisition demand is generated for the first time. If the demand is generated for the first time, the hypertext of the initial screen with the demand is returned to the client side. During the acquisition demand for an interactive identifier, a detector (411) checks whether the information providing object is available, and if available, then the identifier is formed and registered.

The hypertext with the identifier is returned to the client side. When the object is not available, an access rejection message is returned. When the information acquisition demand is added, the interactive identifier is extracted. The propriety of the information is evaluated based on the formation time of the identifier. When the effective term of the identifier has expired, the provision of information is not accepted by a detector (414).

ADVANTAGE - Avoids provision of inaccurate information because of leakage of identifier. Assures security of stored information.

Dwg.2/9

Title Terms: INTERACT; INFORMATION; METHOD; ACCESS; CONTROL; COMMUNICATE; SERVICE; THROUGH; COMPUTER; NETWORK; EVALUATE; INFORMATION; ACCEPT; PROVISION; INFORMATION; EFFECT; TERM; INTERACT; IDENTIFY; EXPIRE

Index Terms/Additional Words: WWW; HTTP

Derwent Class: T01

International Patent Class (Main): G06F-012/00

International Patent Class (Additional): G06F-003/14; G06F-013/00; G06F-015/00

File Segment: EPI

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-146824

(43) 公開日 平成9年(1997)6月6日

(51) Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/00	5 4 7		G 0 6 F 12/00	5 4 7 H
3/14	3 4 0		3/14	3 4 0 A
13/00	3 5 7		13/00	3 5 7 Z
15/00	3 3 0		15/00	3 3 0 Z

審査請求 未請求 請求項の数 2 O L (全 8 頁)

(21) 出願番号 特願平7-307231

(22) 出願日 平成7年(1995)11月27日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 斉藤 典明

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72) 発明者 水澤 純一

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

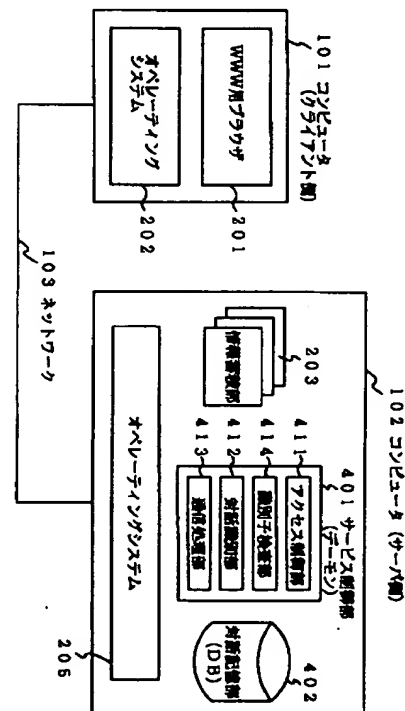
(74) 代理人 弁理士 鈴木 誠

## (54) 【発明の名称】 対話管理型情報提供方法及び装置

## (57) 【要約】

【課題】 同一ユーザからの一連のアクセスを識別する対話識別子に有効期限を設け、漏洩した対話識別子により不正な情報提供が行われるのを防止する。

【解決手段】 クライアント101は、ユーザからの情報取得要求をネットワーク103を通してサーバ102に送り、サーバ102は該要求で示される情報を情報蓄積部203から読み出してクライアント101へ返送する。ここで、サーバ102のサービス制御部(WWWデモン)401は、情報提供対象ユーザを判別する手段411、情報提供対象ユーザに生成日時を付与した対話識別子を発行し、同一ユーザからの一連のアクセスを識別する手段412、対話識別子を提供情報に埋め込み該当ユーザに送信する手段413、及び、対話識別子を検査し、有効期限が過ぎていると情報提供を認めない手段414を有する。



## 【特許請求の範囲】

【請求項1】 情報提供用のWorld-Wide Webを有するサーバコンピュータをコンピュータネットワークでクライアントコンピュータに接続し、HyperText Transfer Protocolにより情報を提供する方法において、クライアント側からの情報取得要求受信時、初回の情報取得要求か、第2回目以降の情報取得要求かを判定し、初回の情報取得要求の場合は、対話識別子の取得要求付情報取得要求をもつ初期画面のハイパーテキストをクライアント側に返送し、

第2回目以降の情報取得要求の時、対話識別子の取得要求の場合は、情報提供対象者であるかどうかを判別し、情報提供対象者の場合、生成日時を明記した対話識別子を生成し、前記対話識別子を登録し、前記対話識別子を付加したハイパーテキストをクライアント側に返送し、情報提供対象者でない場合、アクセス拒否のメッセージを返送し、

対話識別子の付加された情報取得要求の場合は、該情報取得要求内の対話識別子を抽出し、該対話識別子の生成日時に基づき情報提供の可否の判定を行い、対話識別子の有効期限が切れている場合、情報提供を認めないことを特徴とするコンピュータネットワーク上の対話管理型情報提供方法。

【請求項2】 コンピュータネットワークで接続したクライアントコンピュータに対し、World-Wide Webの情報をHyper Text Transfer Protocolにより提供する対話管理型情報提供装置において、情報提供対象のユーザと、情報提供対象でないユーザを判別するアクセス制御手段と、

前記情報提供対象のユーザに、生成日時を付与した対話識別子を発行し、一連のアクセスを識別する対話識別手段と、

前記対話識別子の生成日時を検査し、有効期限を過ぎているとき、前記情報提供対象のユーザに情報提供を行わない識別子検査手段と、

前記対話識別子を提供情報に埋め込み、前記提供情報をユーザに送信する通信処理手段とからなることを特徴とする対話管理型情報提供装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、コンピュータネットワーク上の対話管理型情報提供方法及び装置に関し、詳しくは、ハイパーテキストをコンピュータネットワーク上でユーザに提供するための通信サービスのアクセス制御に関するものである。

## 【0002】

【従来の技術】 従来、ハイパーテキストをコンピュータネットワーク上で、ユーザに対して提供する通信サービスとしWWW (World-Wide Web) が知られており、そのための方法としてHTTP (Hyper Text Trans

fer Protocol) がある。この方法は、不特定多数のユーザへのサービス提供を行うもので、従来は、ユーザのハイパーテキストに対する一連の操作に対して情報取得の要求が生じた時、クライアントコンピュータより、プロトコル、IPアドレス (サーバアドレス)、ポート番号、取得する情報等を、情報取得要求内のURL (Uniform Resource Locator) に設定して、サービス提供元のサーバコンピュータに接続を行い、情報の取得を行っている。

10 【0003】 図6は、従来のこの種のWWWサービスを提供するためのシステム構成例を示したものである。同図において、クライアントコンピュータ101とサーバコンピュータ102はネットワーク (コンピュータネットワーク) 103で接続されている。クライアントコンピュータ101の内部において、201がWWWサービスの提供を受けるための各種ブラウザ、202が該コンピュータ101を制御するための各種オペレーティングシステムである。また、サーバコンピュータ102の内部において、203がWWWサービスでユーザに提供するための情報 (ハイパーテキストなど) の蓄積部、204がWWWサービスを提供するための各種デーモン、205が該コンピュータを制御するための各種オペレーティングシステムである。WWW用ブラウザ201では、該コンピュータ101の入力装置から入力されたユーザからのURLに従い、ネットワーク上のWWWデーモン204に情報取得要求を発行する。情報取得要求を受けたWWWデーモン204では、URLで示される情報蓄積部203内の情報をユーザに転送する。

30 【0004】 図7は、図6のシステム構成におけるクライアントとサーバ間のシーケンスの一例を示したものである。同図において、クライアント側はユーザからの情報取得要求をサーバ (デーモン) 側に送り、サーバ側は、要求された情報を情報蓄積部から読み出してクライアント側に返送する。これをユーザから情報取得要求がある毎に繰り返す。なお、サーバは、複数のユーザから複数回、情報提供要求がある場合でも同様の手順で情報を返送する。

40 【0005】 上記WWWの仕組みは、不特定多数のユーザへの情報提供サービスが対象であり、一連の情報取得要求の中から同一ユーザの識別、ユーザごとの操作履歴の記憶、アクセス履歴により情報の保護等が行えない。

50 【0006】 図8は、従来のWWWサービスを提供するための別のシステム構成例であり、同一ユーザの識別、一連のアクセスの記録、アクセスチェックを可能としたものである。同図において、クライアント側コンピュータ101の内部において、201がWWWサービスの提供を受けるための各種ブラウザ、202が該コンピュータ101を制御するための各種オペレーティングシステムである。一方、サーバ側の102の内部において、203がWWWサービスでユーザに提供するための情報

## 3

(ハイパーテキストなど)の蓄積部、401が対話管理可能なWWWサービスを提供するためのデーモン(ここでは、サービス制御部という)、402が対話管理を行うために必要な情報を蓄積する対話記憶部、205が該コンピュータ102を制御するための各種オペレーティングシステムである。サービス制御部401は、情報提供を行うユーザと提供を行わないユーザを判別するアクセス制御部411、情報提供を行うユーザからの一連のアクセスの識別を行う対話識別部412、ユーザにメッセージの送信を行う通信処理部413からなる。

【0007】ユーザは、情報を提供するサーバへのアクセスの初期の段階において情報提供対象者であることの認証を受け、情報提供対象者には認証を受けた事を示す識別子が発行され、この識別子がユーザへの提供情報に埋め込まれる。以降、ユーザとサーバの間で取り交わされる一連の情報取得要求と提供情報には、この識別子(対話ID)が含まれる。

【0008】図9は、図8のシステムにおけるクライアントとサーバ間のシーケンスの一例を示したものである。クライアント側は、まず(1回目)、ユーザからのURLに従い、サーバ側に情報取得要求を発行する。サーバ側は、この初回の情報取得要求に対し、情報蓄積部203をアクセスし、対話ID取得要求付情報取得要求のURLを発行する初期画面をクライアント側に返送する。これを受けて、次に(2回目)、クライアント側は、対話ID取得要求URLの情報取得要求をサーバ側に発行する。サーバ側は、対話ID取得要求付情報取得要求を判別すると、対話IDを生成し、それを対話記憶部402に登録するとともに、要求のあった情報内のURLに該対話IDを付加してクライアント側に返送する。以後、クライアント側は、URLに対話IDを付加して各種情報取得要求をサーバに発行する。サーバ側は、このURLに付随する対話IDを、対話記憶部402を参照してチェックし、正しければ、情報蓄積部203をアクセスし、URLに対話IDを付加して情報をクライアント側に返送し、対話IDが抽出されないか、該対話IDが対話記憶部402に登録されていない場合は、エラーメッセージなどをクライアント側に返送する。

【0009】上記方法では、対話識別子の導入により、同一ユーザの識別、ユーザごとの操作履歴の記録、アクセス履歴による情報の保護を行うことができ、不特定多数のユーザを対象とした情報提供サービスにおいて高度のアクセス制御が可能であるが、対話識別子が漏洩した場合、該漏洩した対話識別子により不正な情報提供が行われる問題がある。

【0010】

【発明が解決しようとする課題】本発明の目的は、ハイパーテキストをコンピュータネットワーク上で不特定多数のユーザに提供するWWWのHTTPを用いた通信サ

## 4

ービスにおいて、同一ユーザからの一連のアクセスを識別する識別子(対話識別子)が漏洩した場合、それにより不正な情報提供が行われるのを防止することにある。

【0011】

【課題を解決するための手段】本発明は、従来のWWWにおけるHTTPで利用されるURL内の識別子(対話識別子)に、有効期限を設けることを最も主要な特徴とする。

【0012】ユーザからのアクセスの初期の段階において、サーバは、その対話に対する識別子(対話識別子)を生成し、次のアクセスに必要なURLと対話識別子を付加したハイパーテキストをユーザに提供する。この対話識別子には生成日時が記録されている。クライアントは、転送されてきたハイパーテキスト上の所定の文字をユーザがクリックすることにより、対話識別子とURLによってサーバにアクセスを行う。サーバはクライアントから送信されてきた情報取得要求の中の対話識別子を解析し、同一ユーザの識別、一連のアクセスの記憶、所定のアクセスのチェックなどを行う。これらのチェックにおいて、サーバは対話識別子に記録されている生成日時が所定の期間より古いものであれば、当該アクセスを無効とする。これにより、対話識別子の漏洩に備えることができるようになる。

【0013】

【発明の実施の形態】以下、本発明の実施例について図面を参照して説明する。

【0014】図1は、本発明を適用するコンピュータネットワークの一実施例を示したものである。同図において、101はサービスの提供を受けるためにユーザが用いるコンピュータ(クライアントコンピュータ)、102はサービスを提供するためのコンピュータ(サーバコンピュータ)、103は両者の間で通信サービスを提供するためのネットワークである。クライアントコンピュータ101では各種のWWW用ブラウザが動作し、サーバコンピュータ102ではWWWサービスを提供する各種デーモンプログラムが動作し、ネットワーク103を通してユーザに提供するための情報が蓄積されている。なお、実際には、複数のクライアントコンピュータ101がネットワーク103によってサーバコンピュータ102と接続されている。

【0015】図2は、本発明におけるシステム構成の一実施例である。同図において、クライアントコンピュータ101はWWWサービスの提供を受けるための各種ブラウザ201、該コンピュータ101を制御するための各種オペレーティングシステム202からなる。一方、サーバコンピュータ102、WWWサービスにおいてユーザに提供するための情報(ハイパーテキストなど)の蓄積部203、対話管理可能なWWWサービスを提供するためのサービス制御部(デーモン)401、対話管理を行うために必要な情報を蓄積する対話記憶部402、

## 5

該コンピュータ 102 を制御するための各種オペレーティングシステム 205 からなる。ここで、サービス制御部 401 は、情報提供を行うユーザと提供を行わないユーザを判別するアクセス制御部 411、情報提供対象者に発行される識別子を管理する識別子検査部 414、情報提供を行うユーザからの一連のアクセスの識別を行う対話識別部 412、ユーザにメッセージの送信を行う通信処理部 413 で構成される。

【0016】ユーザは、情報を提供するサーバへのアクセスの初期の段階において、アクセス制御部 411 にて情報提供対象者であることの認証を受け、対話識別部 412 にて情報提供対象者には認証を受けたことを示す識別子（対話識別子）が発行され、通信処理部 413 にて、この識別子がユーザへの提供情報に埋め込まれる。以降、ユーザとサーバの間で取り交わされる一連の情報取得要求と提供情報には、この識別子が含まれる。この識別子が識別子検査部 414 にて検査され、一連のアクセスの中で一定期間（例えば 1 日）以上使用された識別子は廃棄（無効にする）する処理が行われる。

【0017】図 3 は、本発明におけるサーバとクライアント間のシーケンスの一例である。これは、ユーザ A の一連のアクセスが 1 日以上経過すると無効となる例を示したものである図 3 において、クライアントは、ユーザ A から URL に従い、サーバに情報取得要求を発行する（1 回目）。サーバは、この初回の情報取得要求に対し、情報蓄積部 203 をアクセスし、ID 取得要求付情報取得要求の URL を発行する初期画面をクライアントに返送する。これを受けて、クライアントは、対話 ID 取得要求付 URL の情報取得要求をサーバに発行する

（2 回目）。サーバは、対話 ID 取得要求付情報取得要求を判別すると、対話 ID を生成し、それを対話記憶部 402 に登録するとともに、要求のあった情報内の URL に該対話 ID を付加してクライアントに返送する。以後、クライアントは、URL に対話 ID を付加して各種情報取得要求をサーバに発行する（3 回目、4 回目、・・・）。サーバは、URL に付随する対話 ID を、対話記憶部 402 を参照してチェックし、正しければ、情報蓄積部 203 をアクセスし、URL に対話 ID を付加して情報をクライアントに返送する。同時に、サーバは対話 ID の有効期限（本例では 1 日）をチェックし、クライアントから該有効期限の切れた対話 ID の付加された情報取得要求が発行されると（n 回目）、エラーメッセージをクライアントに返送する。

【0018】図 4 は、対話識別子を埋め込んだ URL の一例である。始めのアクセスにおいて、初期画面を得るために用いられる一回目のアクセスの URL は従来の WWW と同様である。2 回目のアクセスにおいて、この URL に ID 取得要求が付加される。3 回目以降のアクセスにおいて、クライアントは、各種情報取得要求の他に ID 生成時刻（年月日時分秒：例では 95/05/22

## 6

／11／01／27）を明記した対話 ID を付加してサーバにアクセスを行う。

【0019】図 5 は、図 2 におけるサーバコンピュータ 102 のサービス制御部 401 のフローチャートの一例である。同図において、破線で囲った部分の符号 411～414 は図 2 のサービス制御部 401 内の該当部分 411～414 に対応する。

【0020】ステップ 1001 において、本サーバがクライアントからの要求受付を開始し、ステップ 1002 において、WWW に用いられるブラウザへの URL の入力により、サーバはクライアントより情報取得要求を取得する。ステップ 1003 において、その情報取得要求が初期画面要求（初回アクセス）かどうかを判別し、初期画面要求の場合には、ステップ 1004 において、対話識別子（ID）取得要求の URL が埋め込まれた初期画面をクライアント（WWW ブラウザ）に送信する。

【0021】ステップ 1003 において情報取得要求が初期画面要求でないとは判別された場合には、ステップ 1005 において、情報取得要求の中に識別子取得要求があるかを判別し、識別子取得要求である場合には、ステップ 1006 において、識別子取得要求内のユーザ情報を元に情報提供対象者であるかどうかを判別し、情報提供対象者である場合には、ステップ 1007 において対話識別子を生成し、ステップ 1008 において、対話識別子とユーザ情報を対話記憶部（DB）402 に記録し、ステップ 1009 において、提供する情報の中の URL へ該対話識別子を埋め込み、ステップ 1010 において、その対話識別子の埋め込まれた提供情報を WWW ブラウザへ送信する。ステップ 1006 において、識別子取得要求内のユーザ情報が情報提供対象者でない場合には、ステップ 1017 において、アクセス拒否のメッセージを WWW ブラウザへ送信する。

【0022】ステップ 1005 において情報取得要求の中に識別子取得要求がないとは判別された場合には、即ち、情報取得要求にすでに対話識別子（ID）が付加されている場合は、ステップ 1011 において、情報取得要求内の対話識別子を抽出し、ステップ 1012 において、該抽出した対話識別子の有効期限を検査し、有効期限内であれば、ステップ 1013 において、DB 402 を用い、対話識別子とユーザ情報および情報取得要求により情報提供の可否を判別し、情報提供が許可できる場合には、ステップ 1014 において DB 402 へアクセス記録を残し、ステップ 1015 において、提供情報中の URL へ対話識別子を埋め込み、ステップ 1016 において、その情報を WWW ブラウザに送信する。一方、ステップ 1012 において抽出した対話識別子の有効期限が切れているとは判別された場合には、ステップ 1017 において、アクセス拒否のメッセージが WWW ブラウザに送信される。また、ステップ 1013 における判定結果、情報提供が認められない場合にも、ステップ 10

17においてアクセス拒否のメッセージがWWWブラウザに送信される。

【0023】

【発明の効果】以上説明したように、本発明によれば、一連のアクセスに対する識別子に有効期限を設けることにより、識別子が漏洩した場合においても蓄積情報のセキュリティが確保される効果がある。

【図面の簡単な説明】

【図1】本発明で対象とする通信サービスを提供するためのシステム構成の一例である。

【図2】本発明のサーバコンピュータとクライアントコンピュータのシステム構成の一実施例である。

【図3】本発明におけるサーバとクライアント間のシーケンスの一例である。

【図4】本発明における対話識別子を埋め込んだURLの一例である。

【図5】図2におけるサービス制御部のフローチャートの一例である。

【図6】従来のWWWサービスを提供するためのシステム構成の一例である。

【図7】図6のサーバとクライアントにおけるシーケンスの一例である。

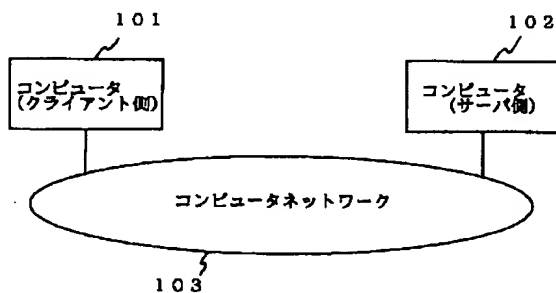
【図8】従来のWWWサービスを提供するためのシステム構成の別の一例である。

【図9】図8のサーバとクライアントにおけるシーケンスの一例である。

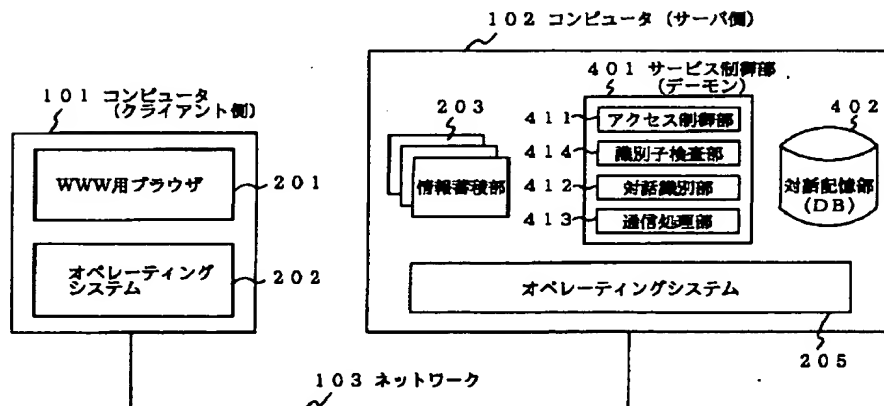
【符号の説明】

- 101 クライアントコンピュータ
- 102 サーバコンピュータ
- 103 ネットワーク
- 201 WWW用ブラウザ
- 202 オペレーティングシステム
- 203 情報蓄積部
- 205 オペレーティングシステム
- 401 サービス制御部
- 402 対話記憶部
- 411 アクセス制御部
- 412 対話識別部
- 413 通信処理部
- 414 識別子検査部

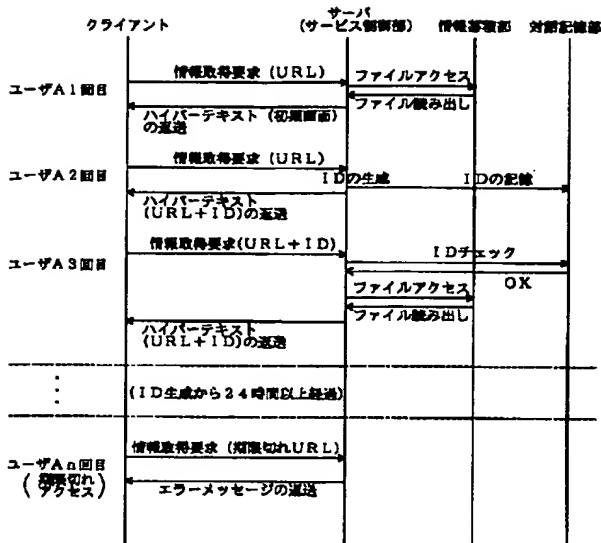
【図1】



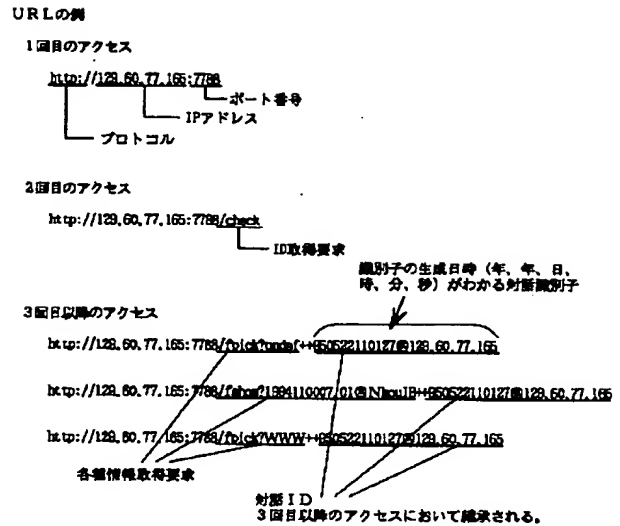
【図2】



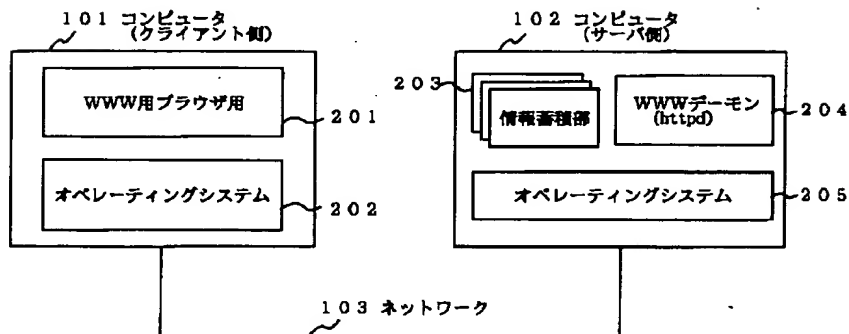
【図3】



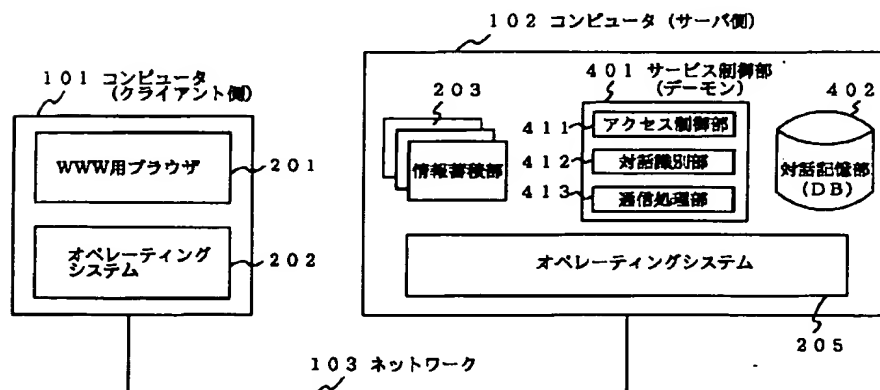
【図4】



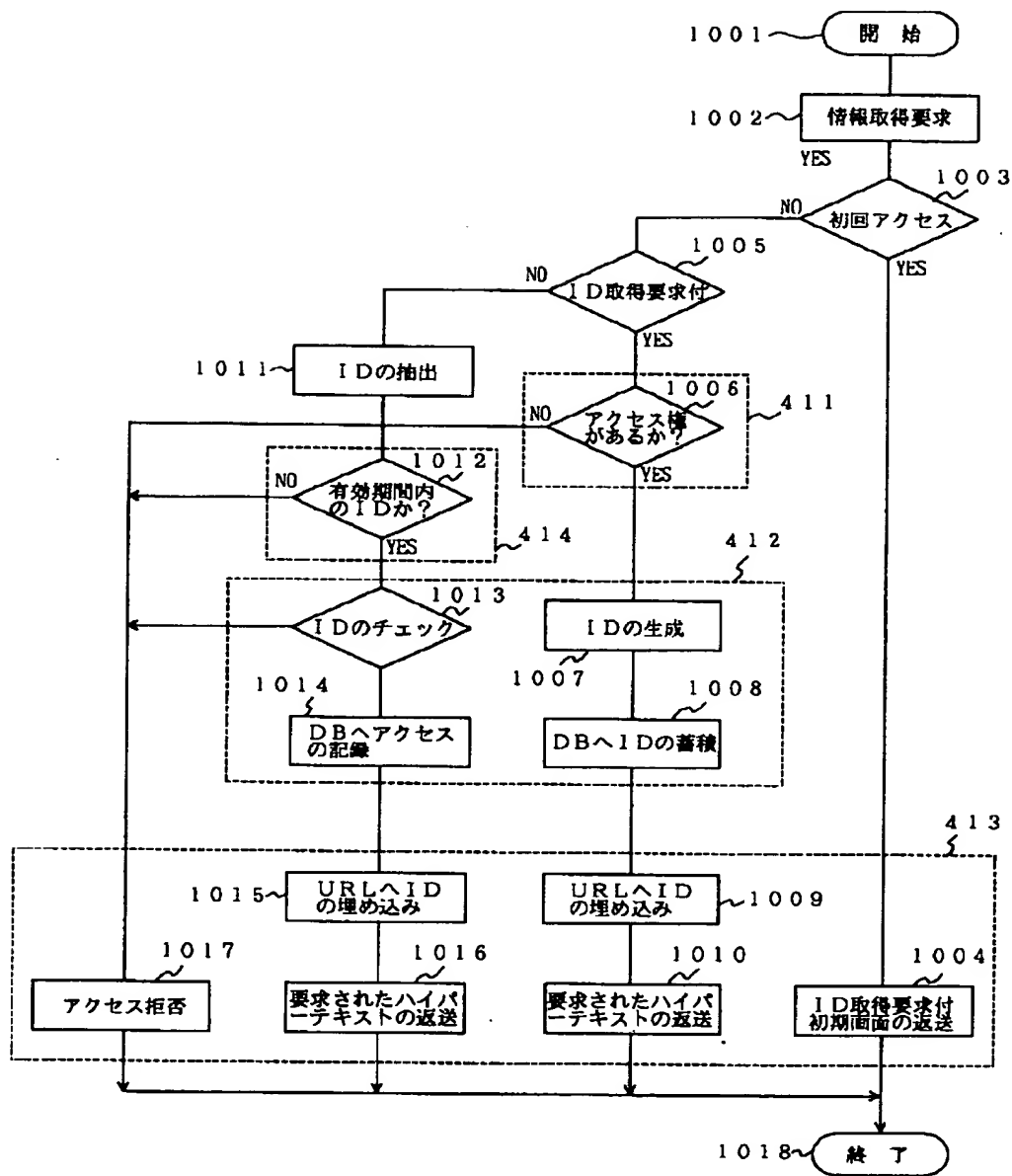
【図6】



【図8】

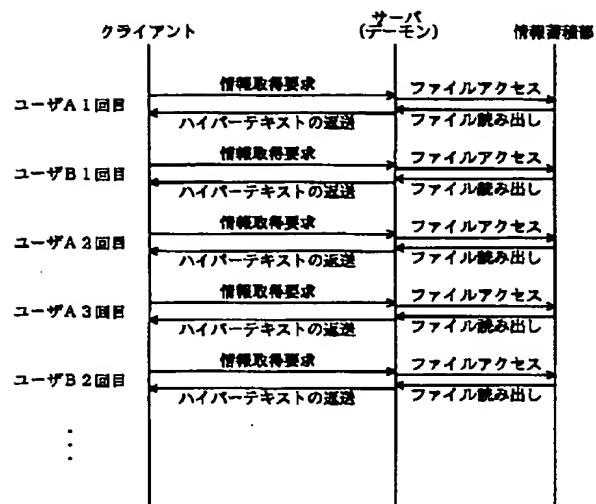


【図 5】





【図7】



【図9】

